Values in Action

Respect ◆ Excellence
Inclusion ◆ Trust
Discovery

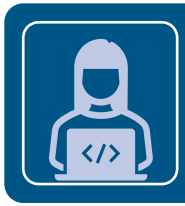
Duke | OFFICE *of* AUDIT, RISK & COMPLIANCE

Annual Report For the Fiscal Year Ended June 30, 2022

Our Mission

The Office of Audit, Risk and Compliance (OARC) talent and resources **advance and integrate** risk awareness, internal controls and compliance requirements; **collaborate** on proactive and innovative improvements to business processes; and **provide high-quality** audit and advisory services to university and health system stakeholders.

Recruit and develop high caliber people



Be leaders within Duke and our profession

Deliver recognized value to our stakeholders

Make important professional contributions

Our People

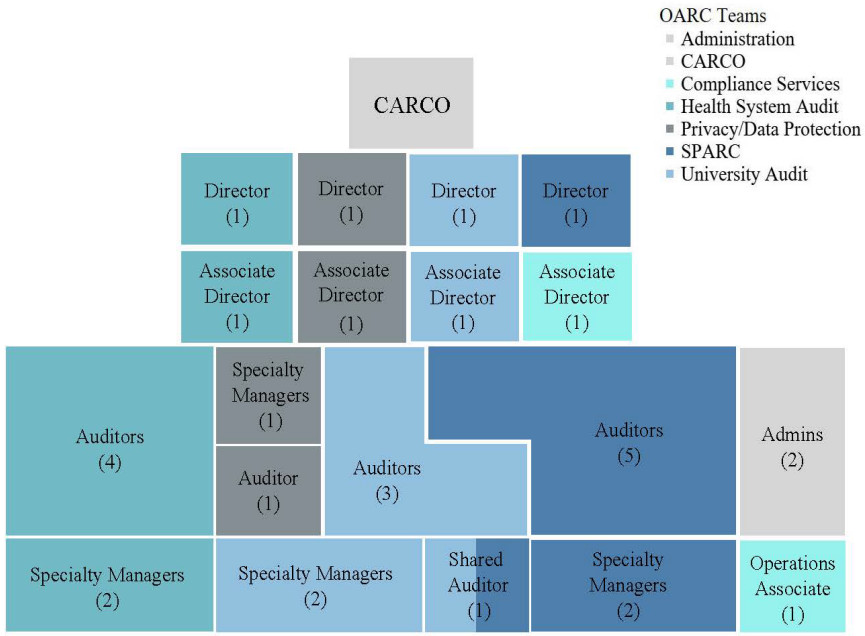
PERSONNEL AND ORGANIZATION STRUCTURE

We focus on hiring high-caliber professionals with proven experience in a combination of audit, compliance and industry settings.

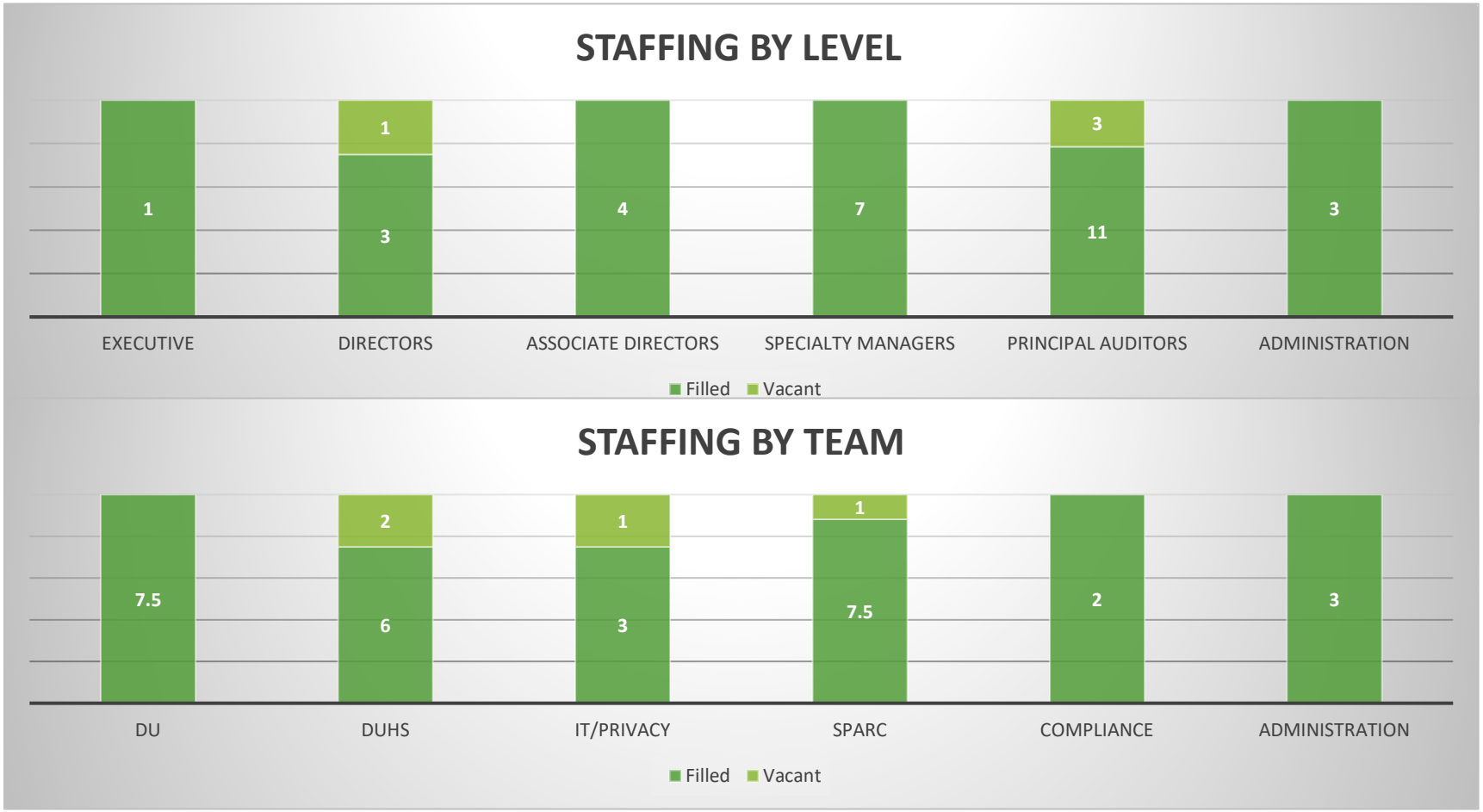
We believe the combination of strategic retention tools and purposeful recruitment of new team members will enable future continuity and staff development.

We value a blend of seasoned professionals who have built knowledge and relationships specific to Duke, as well as those who are less experienced and offer a fresh perspective.

Over the past five years, we converted seven positions to specialty manager or associate director roles to promote continuity in areas that benefit from deeper knowledge: health system IT audit, university IT audit, shared services, clinical research compliance, research program compliance, technology risk assurance and university privacy.



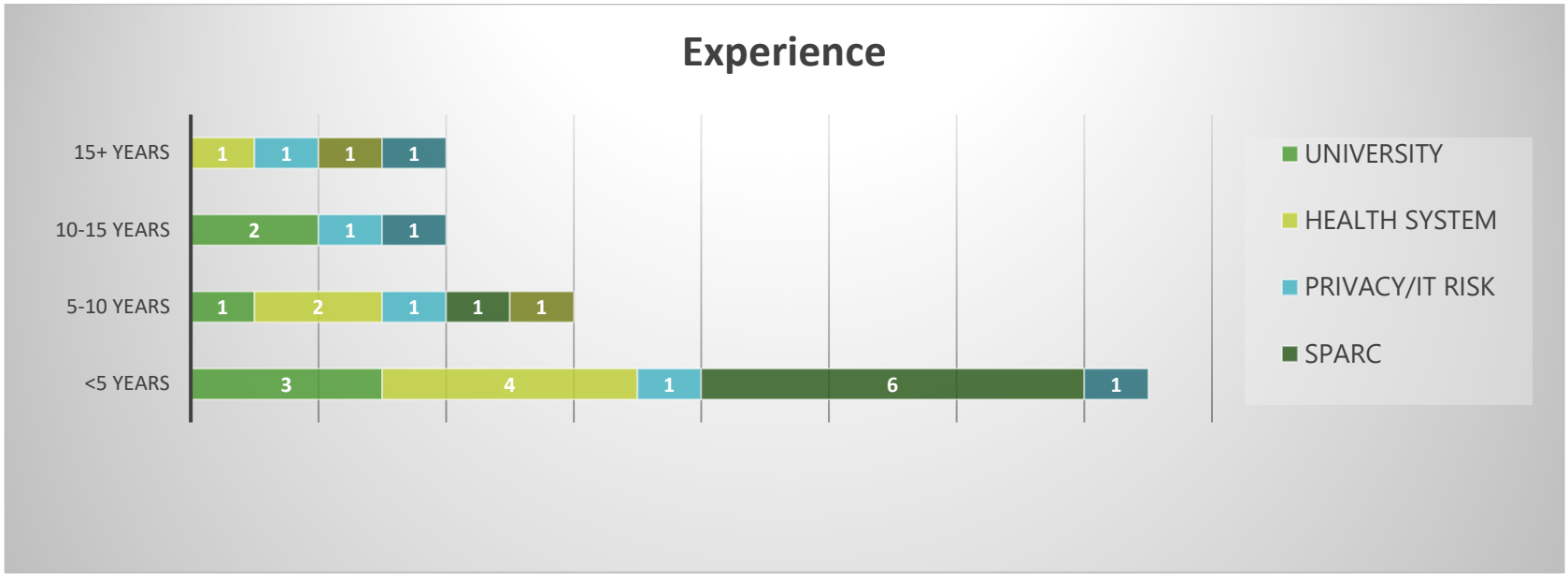
OARC currently has 33 positions serving eight functional areas: university internal audit, health systems internal audit, sponsored programs assurance, university privacy, and institutional programs for IT risk, compliance services, ethics, and enterprise risk management. Please refer to the Appendix or more information on the OARC leadership team.



EXPERIENCE, CREDENTIALS AND PROFESSIONAL CONTRIBUTIONS

OARC hires professionals with a range of experience and expertise. Our principal auditors are often early career professionals who desire development opportunities, while our specialty areas attract experience and subject matter expertise, and our directors bring a combination of proven leadership, talent development and deep subject matter expertise. In all cases, we seek to recruit, retain and promote purpose-driven and highly motivated professionals who want to make meaningful contributions to health care, research and higher education.

Everyone in OARC has a personalized professional development plan that aligns with competencies at each level and with career aspirations. We invest in our people through continuing education opportunities, access to research resources, coaching and mentoring activities, and planned activities to support office culture and team building.

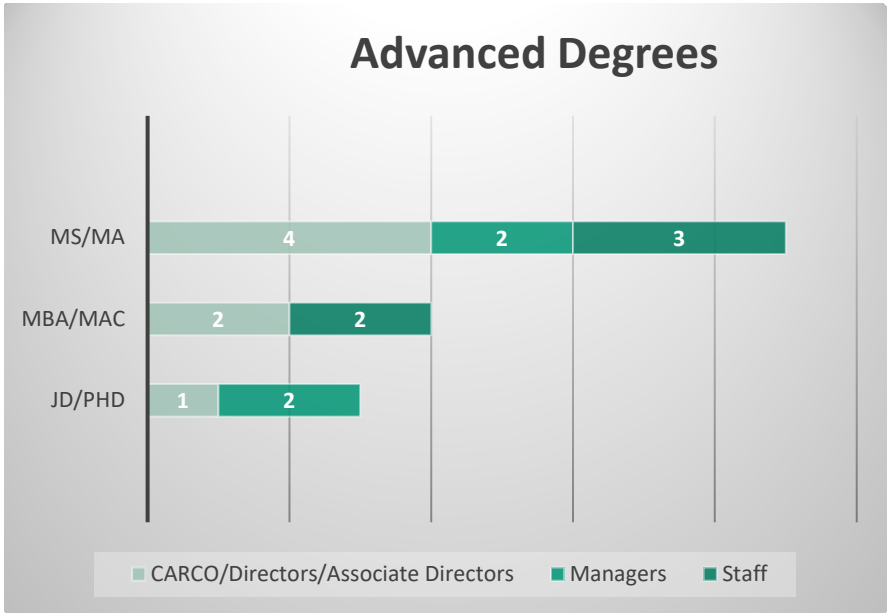


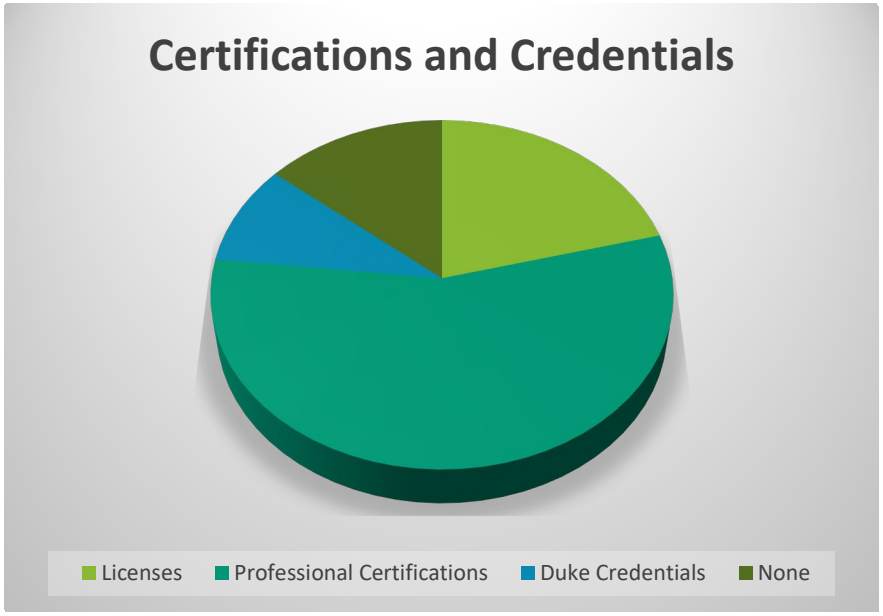
In addition to delivering the assurance, risk and compliance plans, Duke calls on the OARC leadership team to make important contributions to working groups and steering committees. We also share our time and talents with our

professional organizations, industry roundtable meetings and through continuing education training. Through these experiences, we gain insight and knowledge for continuous improvement in the way we assess risks and deliver our services.

Leadership positions in the office require relevant professional credentials, including advanced credentials and/or industry certifications. We encourage all team members to pursue professional credentials and certifications that support career development and specialty knowledge.

Common certifications: Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Duke's Research Costing Compliance (RCC); Duke's Financial Systems Specialist (FSS)





Our Work

KEY GROUP ACCOMPLISHMENTS

Internal Audit

- Senior leadership exposure and collaboration with particular attention on recent personnel transitions
- Performed egagements in right places at the right time, including real-time partnership for emerging risk and controls related to COVID relief funding
- Intentional recruiting with cross training to strengthen staff development and retention

IT Risk and Privacy

- Launched Privacy Impact Assessments to proactively identify ways to improve sensitive information management
- Launched Data Protection Assessments to transition from data risk identification to data governance principles
- Ongoing advisement on impact and implementation of diverse privacy laws and regulations

Sponsored Programs Assurance

- Transitioned routine clinical research directed reviews to a managment monitoring program
- Facilitated engagement with NSOE faculty and staff to streamline and advance research administration processes
- Partnered with the Office of Post Award Financial Management to develop a continuous monitoring program

KEY GROUP ACCOMPLISHMENTS (Continued)

Institutional Compliance

- Ongoing engagement with compliance liasions on action plans to mature compliance functions
- Facilitating discussions on shared compliance responsibilities to help define governance and compliance requirements
- Expanding use of Compliance360 as the institutional policy library

Ethics

- Launched Values in Action as the updated institutional code of conduct and promoting awareness
- Coordinating resource for stakeholders on process improvements for the speak-up program and concern handling
- Expanding use of Compliance360 for institutional case management

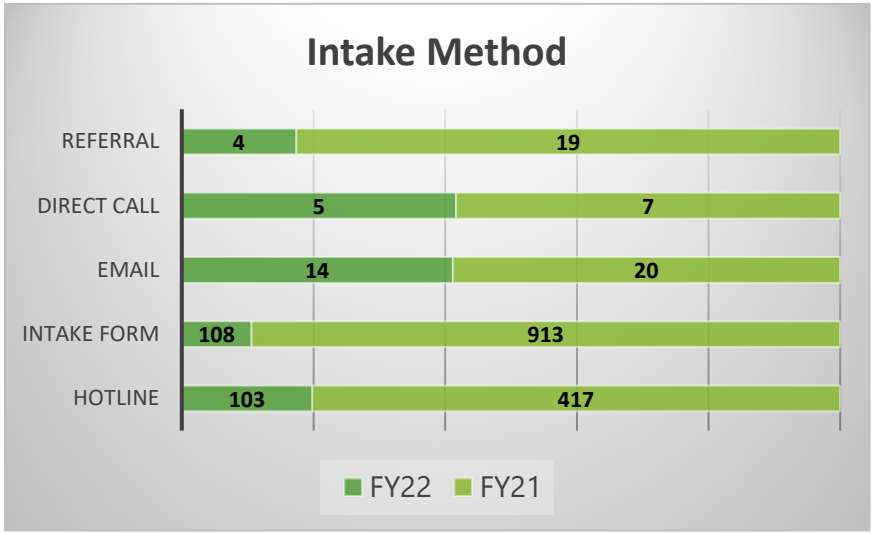
ERM

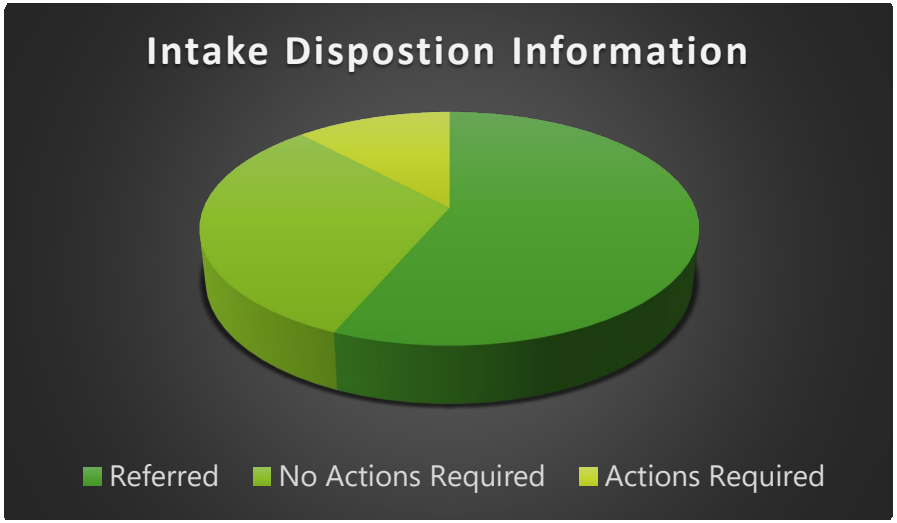
- Created dashboard tracking for all strategic risk priorities
- Established links between strategic risk priorities and governing board visibility
- Ongoing risk awareness discussions, particularly focused on new and high velocity concepts

COMPLIANCE SERVICES HIGHLIGHTS

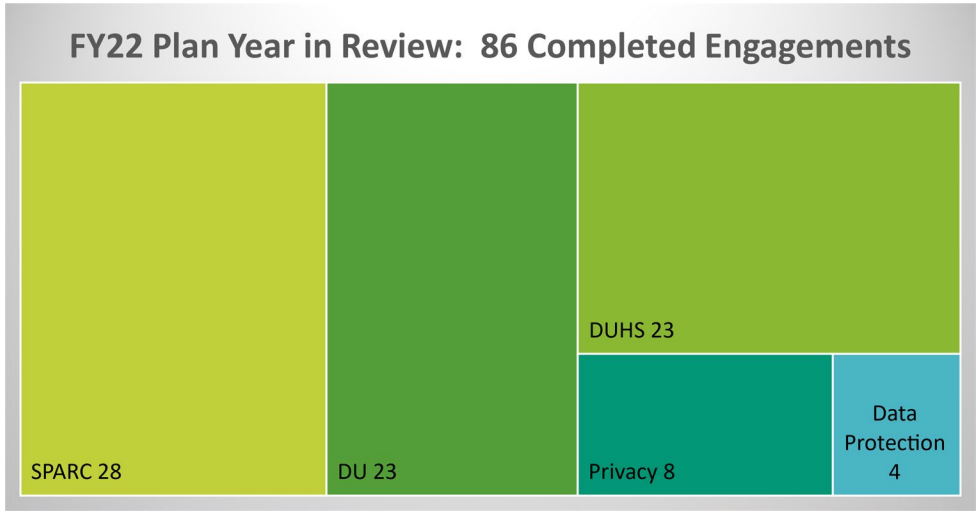
The following charts represent complaints that flowed through OARC Compliance Services reporting channels during FYTD22 and FY21 and were either triaged to other offices or handled directly by OARC.

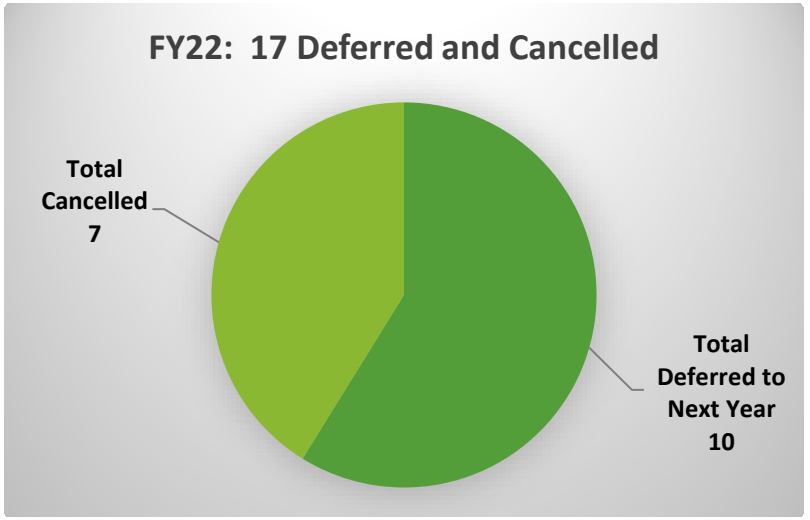
There were 28 cases requiring action by OARC Compliance Services; nine were incidents where OARC performed investigations and issued memos. For the other items, OARC collected additional information and coordinated and hosted meetings or sent emails to connect the relevant departments or to route the incidents appropriately.

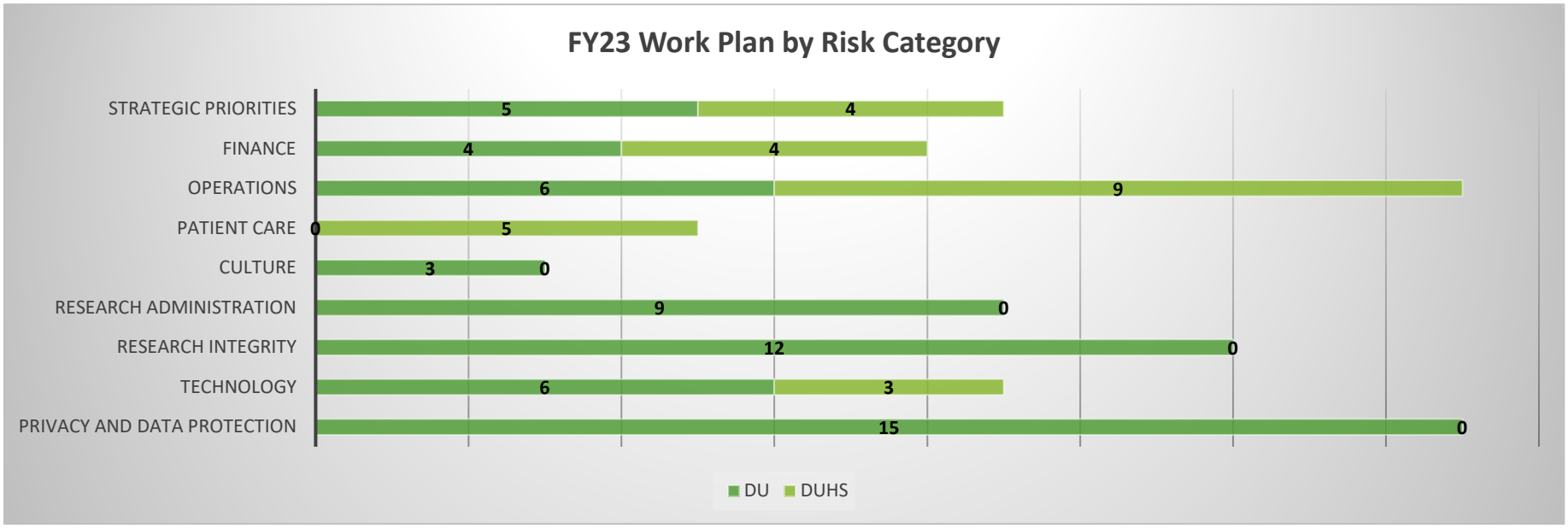




ASSURANCE PROGRAM HIGHLIGHTS





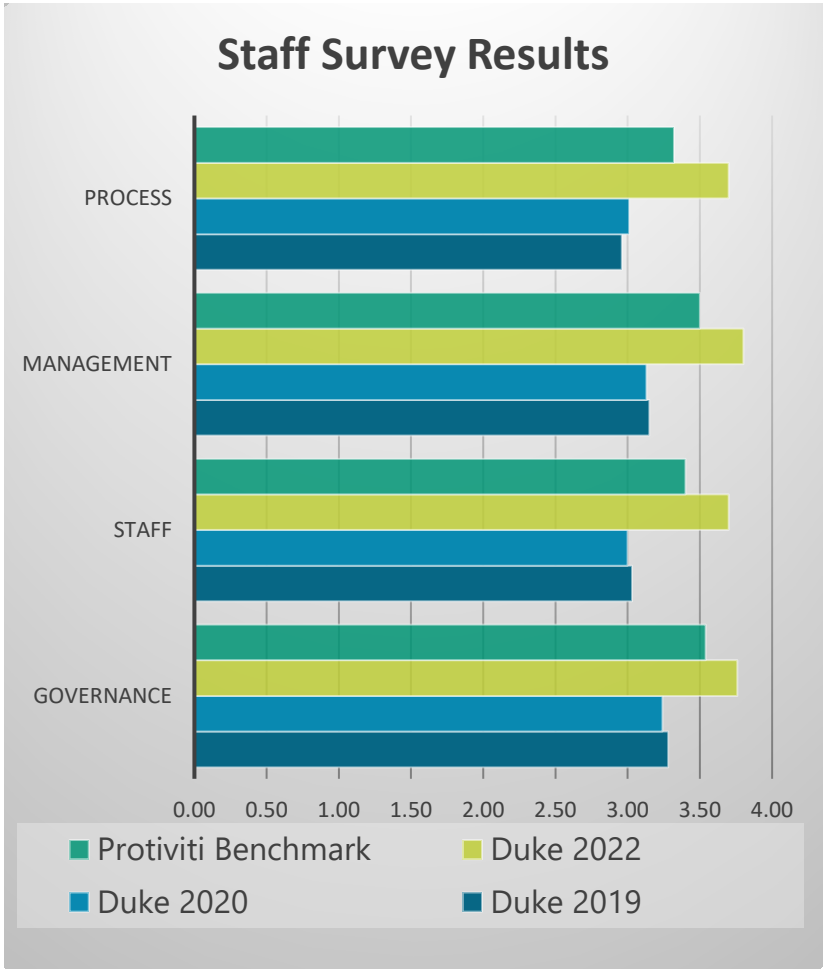


CONTINUOUS IMPROVEMENT

Under professional standards issued by the Institute of Internal Auditors (IIA), a quality assurance review (QAR) is required at least every five years. The 2019 self-assessment and independent validation provided a valuable perspective to ensure OARC is carrying out the mission set forth in the office charter and that we are meeting expectations expressed by management and this committee.

The 2019 QAR report was issued in February 2020. The independent assessment of the internal audit and compliance functions confirmed departmental strengths and made valuable recommendations for continuous improvement. In response to the observations, we committed to action plans to improve and refine our technical practice standards, clarify roles and expectations for our compliance activities, advance team culture and job satisfaction, leverage IT risk assessment in assurance engagement planning, and enhance the university compliance maturity program.

As of FY22, OARC has achieved and sustained all QAR action plans. The most recent staff survey confirms that our staff perceive marked improvement as compared to our 2019 base year and success across all major performance domains.

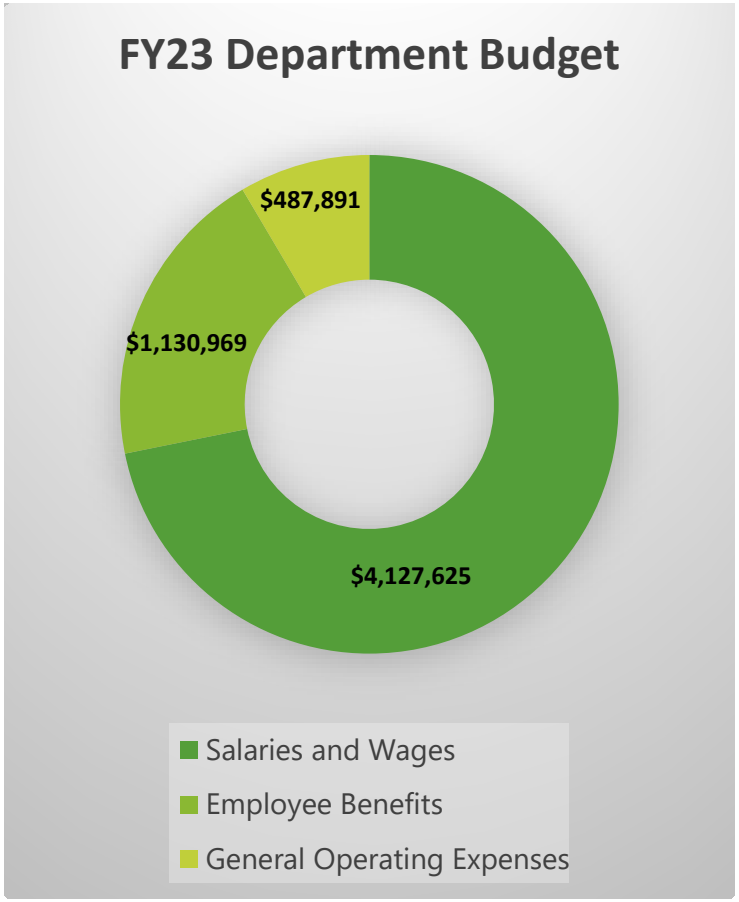


Our Financial Resources

Duke University and Duke University Health System leadership are committed to providing adequate financial resources to support our staffing, professional development, and general operating expenses.

This budget was developed and approved in February 2022 based on known factors and reasonable assumptions at that time. We are confident that the resources we need are either available in the approved budget or would be made available to us as supplemental funding, should the need arise. During fiscal year 2022, Duke authorized out-of-cycle market compensation adjustments for 19 OARC positions, and increased our budget target to reflect the expense increase.

Budget FY23	*$5,746,485*
Budget FY22	*$5,198,467*



Our Future

We are committed to strategic objectives that will guide our focus on five core themes:

- **Operational excellence.** Ensure time, people and resources are efficiently deployed and effectively prepared for the work; this includes careful preparation, focused scope of work, and consistent use of knowledge, experience, data, technology and client goals to inform and deliver the highest quality assurance, compliance and advisory services.

- **Trust and relationships.** Provide transparent, fair, unbiased and informed interactions, engagement and reporting to leadership, colleagues, clients and members of the governing boards; foster intentional and authentic relationships with colleagues and demonstrate genuine interest in their goals and compassionate response to their concerns.

- **Purposeful value.** Combine an in-depth understanding of "why" with an insightful perspective on "how" to validate institutional performance; identify threats to values, compliance, controls, processes and outcomes; and recommend improvements that make Duke better prepared to achieve excellence while balancing risks and benefits.

- **Culture, respect and inclusion.** Value, support and advocate for office and institutional culture that appreciates diverse perspectives, develops professional abilities, grow in knowledge and understanding, rewards accomplishment, and excels based on the drive of every individual to contribute and thrive.

- **Discovery and innovation**. Embrace growth, change and improvement as opportunities to contribute to advancement and achievement; perform research to understand emerging risks and issues and to share findings with others; evaluate options and alternative to achieve excellence; and honor history while moving boldly forward.

APPENDIX: Office Leadership

Leigh P. Goller – Chief Audit, Risk and Compliance Officer. Leigh has institutional responsibility for directing and coordinating integrated internal audit and risk management functions, both of which have enterprise-wide scope; oversight for a federated university compliance function; and accountability to enhance the ability of these functions to advance Duke's mission. Leigh's degrees are in accounting (UNC Charlotte) and liberal studies (Duke), and she is a CPA.

Leigh F. Baxter – Director of Health System Audit. Leigh is responsible for performing the annual risk assessment and development of audit plans. Leigh and the team conduct financial, operational, compliance and IT risk-based audits. Leigh holds a degree in accounting from Florida State University and is a CPA.

Vanessa L. Peoples – Director of Sponsored Programs Assurance and Research Compliance (SPARC). Vanessa's team conducts horizontal assurance reviews aimed at assessing risk and evaluating design effectiveness and efficiency for programs and processes that support sponsored programs administration and clinical research across Duke's research enterprise. Vanessa earned a B.S. in Finance from the University of Delaware and an M.B.A. from North Carolina Central University. She is also a Certified Internal Auditor.

Joanna F. Rojas – Director of University Audit. Joanna leads the university audit team, which provides an independent viewpoint on governance, risk management and internal controls for the university, DUMAC, Inc., and related entities. Joanna and the team conduct financial, operational, compliance and IT risk-based audits. Joanna holds a B.S. from Florida State University and a M.B.A. from Florida Gulf Coast University. Joanna is a Certified Information Systems Auditor. She also serves on the Duke University Federal Credit Union Supervisory Committee.

Privacy and IT Risk Officer. Vacant as of August 2022.

Associate Directors for Internal Audit, Compliance Services and Privacy. Currently, these positions are held by **Ian A. Sterrett** (health system audit), **Kenneth W. Stern** (university audit), **Summer L. Webbink** (compliance services), and **Todd Knowles** (university privacy program). Ian, Ken, Summer and Todd have a combination of external audit experience in public accounting, internal audit experience in corporate and higher education/academic medical center settings, and operational experience for high-functioning privacy programs. Associate directors must have at least eight years of experience with progressive responsibilities as well as certifications, licenses or other designation(s) relevant to the position.